



Return Mail Processing Center
PO Box 9349
Dublin, Ohio 43017

<<Mail ID>>
<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>> <<State>> <<Zip>>
<<Country>>

March 29, 2019

Dear <<Name 1>>:

This letter is to notify you of an incident that may have involved access to your personal information.

What happened? Recently, an employee was tricked via an email phishing scam into opening an attachment/link containing malware - which eventually allowed unauthorized access to individual email account(s). The email account accessed happened to contain some of your personal information.

Phishing scams are very difficult to prevent / detect and are common in the health care industry. The unauthorized person's goal was likely to gain access to employee payroll information (and not necessarily to your information specifically), but because of the way the email account was entered, a copy of the email account was likely unintentionally saved on the outside computer.

There is no evidence that your information specifically has been used inappropriately. However, in an abundance of caution, we thought it best to notify you.

What are we doing? Upon discovery, we blocked the unauthorized access. We then engaged outside technical experts to investigate the incident thoroughly to evaluate the full nature and scope of the access and to identify what information may have been at risk.

Fortunately, this incident was limited to certain employee email accounts, and did not affect our medical record system. Unauthorized access may have first occurred this past November. Experts searched to determine whether sensitive data was located within any of the potentially accessed emails. These same emails were also hand reviewed to obtain names and mailing addresses for use in notification. After completing this extensive review process, on February 19, 2019, we were alerted that some of your information was included within the email account and thereafter sought to notify you.

What information was involved? The email account included your full name and social security number. Additionally, the following information may also have been included in the email account: date of birth/death, addresses, email, telephone number, and other information commonly found in a medical record.

What you can do? To date, there have not been any reports of identity theft or any actual inappropriate use of your specific information related to this incident. However, because we value our relationship with you, we are offering you one (1) year of free credit monitoring and \$1 million in identity theft insurance through Experian to help protect you.

NOTE: You must activate the monitoring product by the activation date in order for it to be effective. The activation instructions and further information on this product are included with this notification. This product is free to you for one (1) year.

We also have included some additional steps that you can take to protect yourself, as you deem appropriate.

For more information about this incident, please call toll free 877-239-1279 between 9 am and 9 pm Eastern Time Monday through Friday. We are fully committed to protecting the confidentiality of the information you provide to us and sincerely apologize for any inconvenience this incident has caused you.

Sincerely,

~~*Christopher Hammond*~~

Vice President, Audit Services

STEPS YOU CAN TAKE

Below is information on steps you can take to protect yourself, if you feel necessary.

- **ACTIVATE Your FREE Experian IdentityWorks product NOW in Three Easy Steps.** To help protect your identity, we are offering you a complimentary one-year membership of Experian's® IdentityWorks® product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.
 1. ENSURE That You Enroll By: **July 5, 2019** (Your code will not work after this date.)
 2. VISIT the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
 3. PROVIDE Your Activation Code: [REDACTED]

If you have questions or need an alternative to enrolling online, please call 877-890-9332 and provide engagement #: [REDACTED]. A credit card is not required for enrollment. Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **\$1 Million Identity Theft Insurance:²** Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the enrollment date (noted above) by enrolling at <https://www.experianidworks.com/3bcredit> or calling 877-890-9332 to register your activation code above in order for this service to be activated. Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer team at 877-890-9332.

- **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze. To place a security freeze on your credit report, contact each of the 3 major consumer reporting agencies -

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax
P.O. Box 105788 Atlanta,
GA 30348 1-800-525-
6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-680-7289
www.transunion.com

To request a freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security Number, and Date of birth; and
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have 3 business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.
- **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it.
- **REPORT** suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)
- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.** Go to <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html>. Federal Trade Commission also provides information at www.ftc.gov/idtheft FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information. (For MD residents: You may contact Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023. For NC residents: You may contact NC Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.
- **FILE YOUR TAXES QUICKLY AND SUBMIT IRS FORM 14039.** If you believe you are at risk for taxpayer refund fraud, the IRS suggests you file your income taxes quickly. Additionally, if you are an actual or potential victim of identity theft, the IRS suggests you give them notice by submitting IRS Form 14039 (Identity Theft Affidavit). This form will allow the IRS to flag your taxpayer account to alert them of any suspicious activity. Form 14039 may be found at <https://www.irs.gov/pub/irs-pdf/f14039.pdf>.
- **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active duty military personnel have additional rights.